SPRINTF

Be careful with string formatting operations.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-17

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 5948 bytes

Attack Category	• Malicious Input
Vulnerability Category	• Format string • Buffer Overflow
Software Context	• String Formatting • String Management
Location	• stdio.h
Description	The sprintf function is used to build strings by embedding format field specifiers in a string and having the data converted into the equivalent string form and then substituted for the specifier. {v}sprintf() is susceptible to buffer overflow if used improperly.Mark any instance of vsprintf() and sprintf() as vulnerabilities. Replace calls with {v}snprintf() or change the format string. Check the format string to see if it includes "%.111s" formatting limit. The return result of sprintf() tells how many characters were actually written. If the number of chars is larger than the original buffer, that means memory has been overwritten and the program state is invalid.
APIs	**Function Name** / **Comments** sprintf — fmt: 1; src: 2 variable; vsprintf — fmt: 1; src: 2 variable; wnsprintf — fmt: 2; src: 3 variable; wnsprintfA — fmt: 2; src: 3 variable; wnsprintfW — fmt: 2; src: 3 variable; wvnsprintf — fmt: 2; src: 3 variable; wvnsprintfA — fmt: 2; src: 3 variable; wvnsprintfW — fmt: 2; src: 3 variable;

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

Method of Attack	Similar to strcpy(), sprintf allows unbounded copying of text, leaving the buffer susceptible to overflow attack. Furthermore, there is no good way to verify that the dest buffer will be big enough for the data to be formatted into it. The general problem is that sprintf does no argument checking internally.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** General: Ensure buffers are null terminated. Insert buffer overflow detection code and if condition is detected, terminate. There is no completely portable manner to address buffer overflow problems with sprintf. Guidance: Convert to snprintf, assuming your platform contains snprintf that is portable. Embed formatting characters for sprintf output.
Signature Details	int sprintf(char *str, const char *format, ...);

Examples of Incorrect Code

```
void main(int argc, char **argv)
{
char usage[1024];
sprintf(usage, "USAGE: %s -f flag
[arg1]\n", argv[0]);
}

/* and then */

/* This subverts the above
apparently safe program */
void main()
{
execl("/path/to/above/program",
<<insert really long string
here>>,
NULL);
}
```

Examples of Corrected Code

```
/* Convert to snprintf */

void main(int argc, char **argv)
{
char usage[1024];
char format_string = "USAGE: %s -
f flag [arg1]\n";
snprintf(usage,
format_string, argv[0], 1024-
strlen(format_string) + 1);
}
```

```
/* Use format string to limit the
amount of characters */
void main(int argc, char **argv)
{
char usage[1024];
sprintf(usage, "USAGE: %.1000s -f
flag [arg1]\n", argv[0]);
}
```

Source References

- Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, pg. 144
- Howard, Michael & LeBlanc, David C. *Writing Secure Code, 2nd ed*. Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228.
- McGraw, Gary & Viega, John. Make Your Software Behave: Preventing Buffer Overflows[2] (2000).

Recommended Resource

Discriminant Set

Operating System	• Windows

Languages	• C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com